REMARKS

In response to the action of September 21, 2007, applicants ask that all claims be allowed in view of the amendments to the claims and the following remarks.

Claims 1-20 are currently pending, of which claims 1, 8 and 13 are independent. Claims 1-7 have been amended, and claim 20 has been added. Support for the new claim may be found in the application, for example at page 7, lines 17-25. No new matter has been introduced.

Claims 1-7 have been rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. In response, applicant has amended claims 1-7. The amendment is believed to address all of the Examiner's concerns. Accordingly, applicant requests reconsideration and withdrawal of this rejection of claims 1-7.

Claims 1-19 have been rejected as being anticipated by U.S. Patent No. 6,578,037 (Wong). Applicant respectfully disagrees that Wong describes or suggests all of the limitations recited by independent claims 1, 8 and 13. For example, and as described more fully below, Wong does not disclose the claimed permission object or using the permission object to determine whether a user associated with an entry in user information is permitted to access a data object associated with a data object type, as recited by claims 1 and 8.

Claim 1 recites a computer-readable medium having embodied thereon a computer program configured to determine whether a user is permitted to access a business object when executing a software application of an enterprise information technology system. The medium includes one or more code segments configured to:

> use a permission object to determine whether a user associated with an entry in user information is permitted to access a data object associated with a data object type, wherein:
>
> the entry in the user information associates the user with a user affiliation,
>
> the permission object identifies:
>
> a user affiliation to which the permission object applies,
>
> a data object type to which the permission object applies such that the data object type is associated with multiple attributes and each data object having the data object type is associated with the multiple attributes,
>
> a permission attribute identifying one of the multiple attributes, and
>
> a permission value for the permission attribute, and
>
> the user is permitted to access the data object when (1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission

> object applies, (2) the data object type of the data object is the same data object type as the data object type to which the permission object applies, and (3) a value of an attribute of the multiple attributes associated with the data object is consistent with the permission value of the permission attribute and the attribute corresponds to the permission attribute.

Instead, Wong discloses techniques to control access to a database by applying different sets of policies for different sets of users. *See* Wong at col. 5, lines 41-43. More particularly, Wong discloses associating a database schema object (which is any object that may be accessed by a user through a database management system) with policy groups, which is a collection of policies. *See* Wong at col. 6, lines 3-6; *see also* col. 5:61-63. A policy in Wong's system is "data, which may include executable code, that reflects rules that govern access to data, such as the data in database schema objects." *See* Wong at col. 5, lines 43-45. Wong provides examples of a policy stating:

> For example, a policy may be a routine or function that generates a predicate to append to a query, such as the system of dynamic predicate attachment described in Lei. The predicate specifies conditions that restrict results returned by a query, thereby restricting access to data.

Wong at col. 5, lines 46-49. Wong provides examples of access rules:

> Specifically, policy functions 162 and 164 reflect access rules for users who are persons in the Human Resource department of Company A accessing database schema object 104. Those access rules may, for example, permit users in Human Resources of Company A to access employee records of employees earning salaries below a threshold. Policy functions 172 and 174 reflect access rules for users who are persons in the Human Resources department of Company B. Access rules to database schema object 104 for Company B are not based on the salary of employees. Rather, the access rules of Company B, for users in the Human Resources Department permit those users to access employee records of employees who belong to particular job categories.

Wong at col. 6, lines 26-39 (emphasis added); *see also* Wong at Fig. 1.

Wong discloses techniques whereby access to a database schema object are controlled by one or more collections (called a policy group) of policies (or policy functions), where a policy reflects access rules (which may be executable code, a routine or a function). *See* Wong at col. 5, lines 41-45 and 61-63 and col. 6, lines 26-39.

In contrast to Wong's access rules, claim 1 recites using a permission object to determine whether a user … is permitted to access a data object associated with a data object type, where the permission object identifies (1) a user affiliation to which the permission object applies, (2) a data object type to which the permission object applies such that the data object type is associated with multiple attributes and each data object having the data object type is associated

with the multiple attributes, (3) a permission attribute identifying one of the multiple attributes associated with the data object type, and (4) a permission value for the permission attribute. As noted above, claim 1 recites using a permission object to determine whether a user … is permitted to access a data object associated with a data object type. More particularly, claim 1 recites that the user is permitted to access the data object when (1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies, (2) the data object type of the data object is the same data object type as the data object type to which the permission object applies, and (3) a value of an attribute of the multiple attributes associated with the data object is consistent with the permission value of the permission attribute and the attribute corresponds to the permission attribute.

In contrast to using a permission object to determine whether a user … is permitted to access a data object associated with a data object type, as recited by claim 1, Wong discloses:

> To determine whether a particular policy group should limit a user's access to data, DBMS 100 needs information about the user that may be used to determine what policy groups to apply to the user. Context information 130 is information associated with a user that is maintained or accessed by DBMS 100. Context information 130 contains a policy group attribute 132. A policy group attribute, such as policy group attribute 132, is an attribute or data element in Context information that identifies which policy group should apply. Preferably, a policy group attribute is an attribute which may be securely set by DBMS 100 in response to messages from an application, and may therefore be trusted by the database system and relied upon to determine what policy groups to apply.
>
> One mechanism for associating a policy group attribute value with a user involves using the user context attribute values described in Lei. User context attribute values are associated with a user session, and are established when the user session is established. A session is a specific connection of a user to a database server via a user process. Upon establishing a session, DBMS 100 stores information, typically in memory, that pertains to the session. The information maintained includes the user context attribute values stored in association with a session of user 210.

Wong at col. 6, line 51 to col. 7, line 7.

The action contends that Wong's policy group attribute corresponds to the claimed permission object. See action at page 3, lines 8-10. Applicant respectfully disagrees. Even assuming only for the sake of argument that the action's correspondence is correct, Wong's policy group attribute does not describe or suggest the claimed permission object. As noted above, the permission object identifies (1) a user affiliation to which the permission object applies, (2) a data object type to which the permission object applies such that the data object type is associated with multiple attributes and each data object having the data object type is

associated with the multiple attributes, (3) a permission attribute identifying one of the multiple attributes associated with the data object type, and (4) a permission value for the permission attribute, as recited by claim 1. Wong's "policy group attribute, such as policy group attribute 132, is an attribute or data element in Context information that identifies which policy group should apply." Wong at col. 5, line 57-60. Wong's policy group attribute does not describe or suggest a permission object having, among other features, a permission attribute identifying one of the multiple attributes associated with the data object type, and a permission value for the permission attribute, as recited by claim 1.

As best understood, the action also contends that Wong's disclosure of access rules that permit some users to access employee records of employees earning salaries below a threshold and other access rules permit other users to access employee records of employees who belong to particular job categories discloses a permission object having a permission attribute identifying one of the multiple attributes associated with the data object type, and a permission value for the permission attribute. Applicant respectfully disagrees. As noted previously, Wong uses access rules which are reflected in a policy, which may be executable code, a routine or function. Hence, Wong does not describe or suggest using a permission object to determine whether a user … is permitted to access a data object associated with a data object type, where the permission object identifies (1) a user affiliation to which the permission object applies, (2) a data object type to which the permission object applies such that the data object type is associated with multiple attributes and each data object having the data object type is associated with the multiple attributes, (3) a permission attribute identifying one of the multiple attributes associated with the data object type, and (4) a permission value for the permission attribute, as recited by claim 1.

Accordingly, applicant respectfully requests reconsideration and withdrawal of the rejection of claim 1 and its dependent claims 2-7.

Independent claim 8, although different in scope from claim 1, recites features similar of those in claim 1 discussed above. Accordingly, applicant respectfully requests reconsideration and withdrawal of the rejection of claim 8 and its dependent claims 9-12.

Independent claim 13 recites a computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise

information technology system. The system includes a data repository for access control information for software and an executable software module. The data repository has data objects, where each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each attribute of the multiple attributes.

The data repository includes:

> user information that associates a user affiliation with a user of the software application, and
>
> permission information having multiple permission objects, each permission object identifying a user affiliation to which the permission object applies, a data object type to which the permission object applies, a permission attribute identifying one of the multiple attributes, and a permission value for the permission attribute.

The executable software module causes:

> a comparison of a value of an attribute of the multiple attributes associated with a data object to which a user seeks to access such that the attribute corresponds to the permission attribute of a permission object with the permission value of the permission object, and
>
> an indication that a user is permitted to access a data object when the value of the attribute associated with the data object is consistent with the permission value of the permission object.

In contrast and as noted above, Wong discloses techniques whereby access to a database schema object are controlled by one or more collections (called a policy group) of policies (or policy functions), where a policy reflects access rules (which may be executable code, a routine or a function). *See* Wong at col. 5, lines 41-45 and 61-63 and col. 6, lines 26-39. As discussed above, Wong does not describe or suggest permission objects as recited by claims 1 and 8.

Accordingly, for at least the reasons discussed above with respect to claim 1, applicant respectfully requests reconsideration and withdrawal of the rejection of claim 13 and its dependent claims 14-19.

New claim 20 depends from claim 1 and is similarly distinguishable from Wong. Furthermore, the applied art fails to disclose or suggest at least some of the additional features recited in the new dependent claim. For at least these reasons, applicant accordingly submits that claim 20 is in condition for allowance.

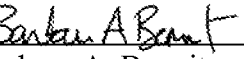
Applicant submits that all claims are in condition for allowance.

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

The fee in the amount of $460 for the two-month extension of time is being paid concurrently herewith on the Electronic Filing System (EFS) by way of Deposit Account authorization. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: February 20, 2008



Barbara A. Benoit
Reg. No. 54,777

Customer No. 26171
Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331